Hermann Minkowski : des formes quadratiques à la géométrie des nombres

Sebastien Gauthier

Hermann Minkowski : des formes quadratiques à la géométrie des nombres

Le 12 octobre 2009, par **Sébastien Gauthier**

Maître de Conférences à l'Institut Camille Jordan, Université Lyon 1 (**page web**)

Dans cet article, on présente un théorème de Minkowski (1864-1909) qui est emblématique d'une théorie fondée par ce mathématicien : la géométrie des nombres. Considéré par Minkowski comme géométrique, ce théorème fut néanmoins élaboré à l'origine pour étudier des problèmes arithmétiques.

LA *géométrie des nombres* est un domaine des mathématiques relevant de la *théorie des nombres*. Elaborée à la fin du XIXème siècle par le mathématicien allemand *Hermann Minkowski*, la géométrie des nombres se caractérise à l'origine par l'adoption d'un point de vue géométrique pour étudier des phénomènes arithmétiques, c'est-à-dire des propriétés des nombres entiers. Il s'agit d'un sujet de recherche encore actif actuellement. Les recherches contemporaines approfondissent des thèmes déjà abordés par Minkowski [**1**], mais un nouvel intérêt pour la géométrie des nombres est né de ses applications à l'informatique. Depuis le début des années 1980, des questions *algorithmiques* liées à la géométrie des nombres sont utilisées en *cryptologie* [**2**].

Quand Minkowski développe ce sujet à la fin du XIXème siècle, il s'intéresse à des problèmes classiques de la théorie des nombres de cette époque, problèmes qui concernent ce que les mathématiciens appellent alors la *théorie arithmétique des formes*. Nous verrons sous peu de quoi il s'agit, mais nous nous tournerons dans un premier temps vers Minkowski lui-même.

Éléments biographiques sur Minkowski

Hermann Minkowski est né le 22 juin 1864 à Alexotas [**3**] en Russie de parents allemands. Il est le quatrième d'une famille de cinq enfants. Oskar, un de ses frères qui est médecin, est aussi un scientifique célèbre pour des travaux portant sur le diabète. En 1872, la famille s'installe à Königsberg où Hermann Minkowski fait de brillantes études secondaires. Suivant les conseils d'un de ses professeurs, il contacte Heinrich Weber alors professeur de mathématiques à l'université de Königsberg. Un commentaire dans une lettre à Richard Dedekind [**4**] montre que ce dernier est impressionné par les connaissances du jeune lycéen :

> « Je veux t'écrire à cette occasion à propos d'un génie mathématique, et particulièrement arithmétique, qui a fait son apparition ici et qui promet beaucoup. C'est un élève de Terminale du lycée local qui n'ira à l'université que dans un an et s'est plongé complètement de sa propre initiative dans l'analyse supérieure et dans la théorie des nombres, qu'il a étudié d'après la première édition de tes Cours de Dirichlet [5]. Maintenant, il pense faire les *Disquisitiones* [6]. »

Minkowski entre à l'université en 1880. Il étudie essentiellement à Königsberg et, pour trois semestres, à l'université de Berlin. Il suit surtout des cours de mathématiques, mais il montre déjà son intérêt pour la physique (il assiste par exemple à des cours de mécanique et de statique). C'est aussi pendant cette période à l'université de Königsberg qu'il rencontre David Hilbert (lui aussi étudiant) et Adolf Hurwitz (alors jeune professeur) avec qui il restera ami par la suite.

Minkowski se fait connaître de la communauté mathématique en 1883, alors qu'il n'est encore qu'étudiant, en remportant le Grand Prix de l'Académie des sciences. L'attribution de ce prix fit scandale pour plusieurs raisons. L'une d'elles, c'était que le problème proposé par l'Académie (déterminer le nombre de décompositions d'un entier en somme de cinq carrés) avait déjà été résolu en 1867 par un professeur d'Oxford : Henry J.S. Smith. Ce dernier reçoit le prix à titre posthume au même titre que Minkowski, mais cela ne suffit pas à faire taire les critiques envers les académiciens français [7].

Minkowski obtient son doctorat en juillet 1885, avec, pour sujet de recherche, la théorie des nombres et, plus précisément, la théorie arithmétique des formes quadratiques. Après son service militaire, il commence sa carrière universitaire à l'université de Bonn en 1887, et il y continue ses recherches en mathématiques. Il se tourne également vers la physique avec des travaux sur la mécanique et l'hydrodynamique. Minkowski quitte Bonn en 1894 pour revenir à Königsberg ; puis en 1896, il accepte un poste de professeur à l'Ecole Polytechnique de Zürich, avant de rejoindre, en 1902, son ami Hilbert à l'université de Göttingen. Minkowski y poursuit son travail en mathématiques tout en étant aussi très actif en physique : il conduit un séminaire de physique en collaboration avec Hilbert, et les thèmes abordés à partir de 1905 l'amènent à s'intéresser à la théorie de la relativité. Lors d'une conférence intitulée *espace et temps* en septembre 1908 à Cologne, il développe l'idée d'un espace-temps de dimension 4. Minkowski décède à Göttingen, peu de temps après, le 12 janvier 1909, d'une crise d'appendicite.

La théorie arithmétique des formes quadratiques

Une part importante des contributions mathématiques de Minkowski concerne ce qu'il baptise lui-même la *géométrie des nombres*. Les recherches de Minkowski sur ce thème doivent être replacées dans la continuité des travaux qu'il avait effectués pour le prix de l'Académie aussi bien que pour sa thèse et qui concernaient la théorie arithmétique des formes quadratiques. La géométrie des nombres est une nouvelle approche pour cette théorie et elle se caractérise par le fait que la géométrie occupe une place centrale. De quoi s'agit-il ?

Revenons à la question de la décomposition d'un entier en sommes de carrés. Par exemple, on peut interpréter le problème de déterminer si un entier naturel p est la somme de deux carrés comme la recherche de deux entiers x et y qui vérifient la relation

$$p = x^2 + y^2.$$

Le problème peut donc se ramener à la question de trouver les solutions entières de l'équation $p = x^2 + y^2$. Une forme quadratique est une expression qui généralise une somme de carrés de ce type. Par exemple, lorsqu'il y a deux variables comme c'est le cas ici, on parle de formes quadratiques *binaires* et celles-ci s'écrivent de façon générale

$$ax^2 + 2bxy + cy^2.$$

Lors des premiers travaux consacrés à ces formes au XVIIIème siècle et au début du XIXème siècle, les coefficients a, b, c étaient des nombres entiers. Le problème de la théorie arithmétique des formes est de déterminer les nombres entiers p qui sont « représentables » par une forme, c'est-à-dire pour lesquels il existe des valeurs entières des variables x et y telles que p peut s'écrire sous la forme :

$$p = ax^2 + 2bxy + cy^2.$$

Le problème précédent se généralise à un nombre quelconque de variables et, à une somme de n carrés $x_1^2 + x_2^2 + \cdots + x_n^2$, on peut faire correspondre une forme quadratique de n variables [8].

Dans les *Disquisitiones Arithmeticae*, Gauss s'intéresse à la représentation des entiers par une forme quadratique. Il essaie alors de déterminer les différentes formes qui représentent exactement les mêmes nombres entiers. Pour cela, il introduit la notion d'équivalence entre formes. Pour Gauss, les formes équivalentes doivent avoir la propriété de représenter les mêmes nombres entiers. Il définit alors l'équivalence de la manière suivante : deux formes quadratiques binaires $ax^2 + 2bxy + cy^2$ et $a'x'^2 + 2b'x'y' + c'y'^2$ sont équivalentes si on peut passer de l'une à l'autre par un changement de variables du type

$$\begin{cases} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{cases},$$

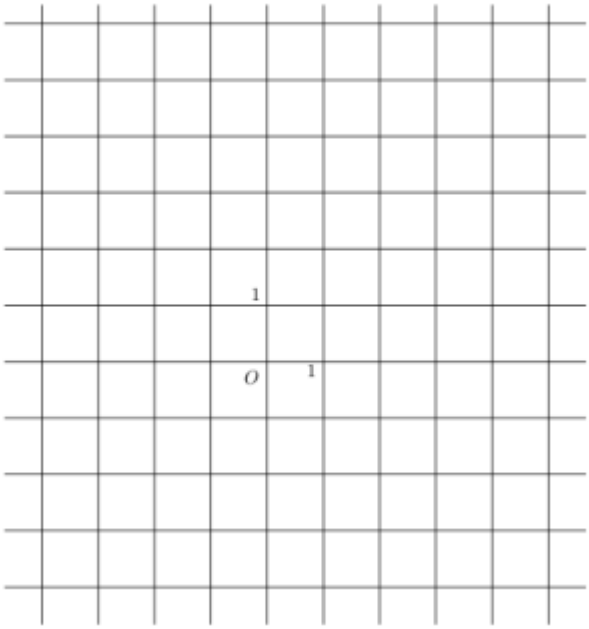
où α, β, γ et δ sont des entiers qui vérifient $\alpha\delta - \beta\gamma = \pm 1$. Ainsi définies, deux formes équivalentes représentent bien les mêmes entiers, mais attention la réciproque est fausse : des formes représentant les mêmes nombres ne sont pas toujours équivalentes. L'ensemble des formes équivalentes entre elles s'appelle une classe.

Gauss veut ensuite définir une forme privilégiée parmi une classe de formes équivalentes, ou encore choisir une forme qui représente toutes celles d'une même classe. Une telle forme, appelée forme réduite, doit avoir des propriétés particulières permettant de l'identifier parmi toutes les autres formes de sa classe, et cela (si possible) de manière unique. Une forme réduite est caractérisée par des inégalités qui sont vérifiées par ses coefficients. Gauss résout ce problème pour les formes quadratiques binaires définies positives, c'est-à-dire celles qui ne prennent que des valeurs strictement positives quand les variables x, y sont toutes les deux non nulles [9]. La question de la réduction, puis sa généralisation aux formes de plus de deux variables, sont délicates. De nombreux mathématiciens s'y intéressèrent au cours du XIXème siècle. C'est sur ce problème que Minkowski travaille, à la fin des années 1880 et au début des années 1890, quand ses idées sur la géométrie des nombres commencent à apparaître dans ses publications et dans sa

correspondance avec Hilbert. Il considère alors des formes à coefficients réels et de n variables. Elles sont donc plus générales que celles qu'envisageaient les mathématiciens du début du siècle, et le problème de la réduction se pose aussi à leur sujet. Minkowski étudie en fait un problème lié à celui de la réduction : il cherche à déterminer les plus petites valeurs prises par la forme, quand ses variables sont des entiers non tous nuls, ou, tout au moins, à estimer ce minimum. C'est pour répondre à cette question que Minkowski développe la géométrie des nombres, dont le résultat central (le théorème dit de Minkowski) fournit ce type d'estimation.

Le théorème de Minkowski

On considère, dans le plan, un repère orthonormé d'origine O. Soit le réseau L des nombres entiers [10] (on peut penser à un quadrillage dont la maille est un carré, comme le montre la figure 1) et $\mathcal{R}$ une partie centrée en O (cela signifie que $\mathcal{R}$ admet O comme centre de symétrie), convexe [11] et dont l'aire est plus grande que 4.
Minkowski établit alors qu'*il y a au moins un point du réseau L, différent de l'origine O, qui se trouve à l'intérieur de $\mathcal{R}$ ou sur son bord*.

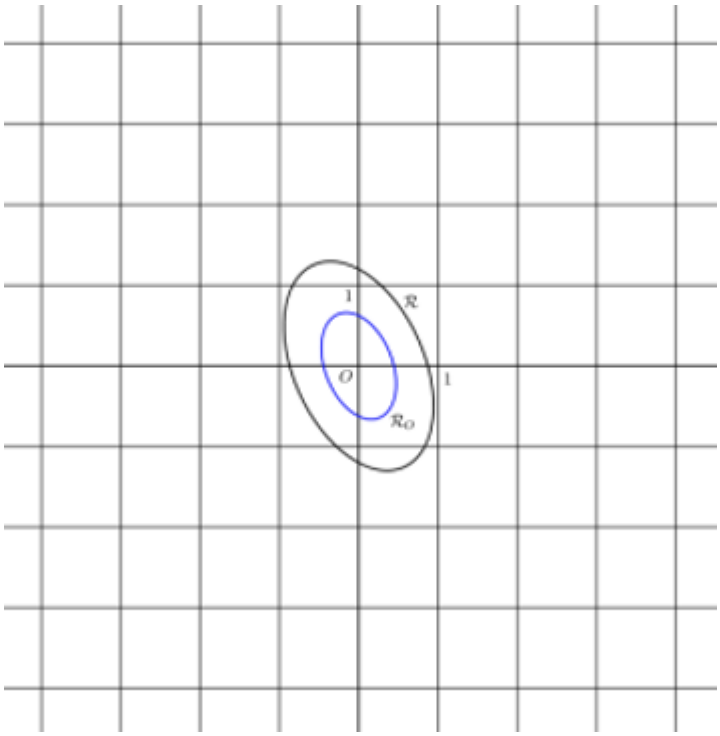


Si, pour simplifier, on choisit pour $\mathcal{R}$ un disque de centre O, ce théorème exprime le fait que, lorsque le cercle est suffisamment grand, il contient nécessairement des points du quadrillage autres que O. Par exemple, un disque dont l'aire est 4 a un rayon égal à $\frac{2}{\sqrt{\pi}}$. Le rayon étant strictement plus grand que 1, ce cercle contient le point de coordonnées $(1,0)$.

En 1891, dans une conférence à Halle, Minkowski propose pour la première fois un énoncé de son théorème. Il le donne alors en dimension 3. Mais comme il le montre dans la suite de son travail, ce résultat se généralise en dimension quelconque (l'aire doit alors être remplacée par le volume et le $4 = 2^2$ par 2^n pour la dimension n) et pour n'importe quel réseau constitué de parallélogrammes de volume égal à 1 [12].

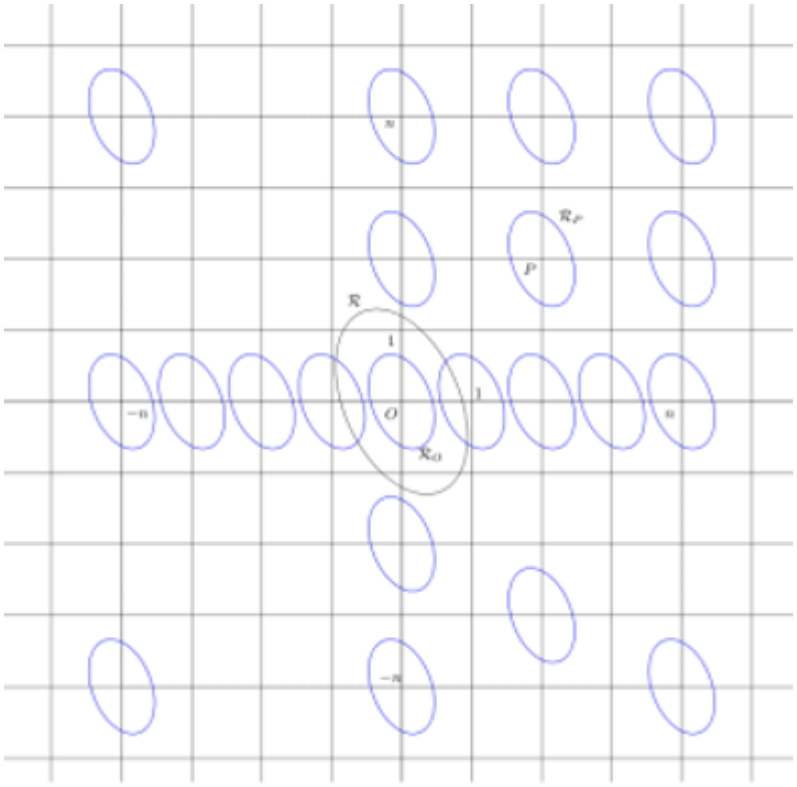
Revenons à l'énoncé en dimension 2 pour expliquer les grandes lignes de la démonstration [13].

On suppose d'abord que l'aire de $\mathcal{R}$ est strictement supérieure à 4. La première étape consiste à considérer la partie $\frac{1}{2}\mathcal{R}$ (notée $\mathcal{R}_O$) : le même domaine que $\mathcal{R}$ mais de taille moitié dans toutes les directions [**14**] (voir la figure 4) !

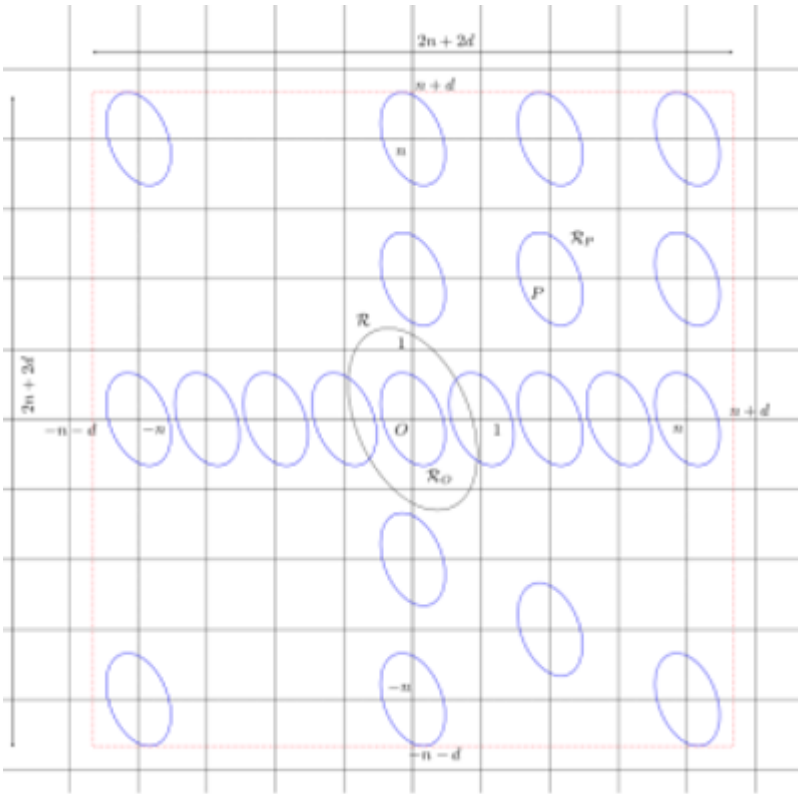


Comme l'aire de $\mathcal{R}$ est strictement plus grande que 4, celle de $\mathcal{R}_O$ est strictement supérieure à 1.

La partie $\mathcal{R}_O$ est ensuite reproduite autour de chaque point du réseau. On note $\mathcal{R}_P$ la partie centrée au point P du réseau. L'objectif est maintenant de montrer qu'il y a nécessairement au moins deux de ces parties $\mathcal{R}_P$ qui se rencontrent (voir la figure 5 où quelques domaines $\mathcal{R}_P$ sont représentés).



Pour cela, on considère les parties $\mathcal{R}_P$ pour des coordonnées de P comprises entre $-n$ et n, où n est un entier naturel. On prend donc toutes les $\mathcal{R}_P$ dont les centres se trouvent dans un carré de côté $2n$. On augmente alors légèrement la longueur de chaque côté de ce carré pour obtenir un nouveau carré de côté $2n + 2d$ qui contient toutes les parties construites à l'étape précédente (voir la figure 6).



Cette construction doit permettre de montrer que les parties $\mathcal{R}_P$ doivent nécessairement se rencontrer. L'idée est de remarquer que, si ce n'était pas le cas, les parties $\mathcal{R}_P$ prendraient moins de place que le carré qui les contient. En effet, si les $\mathcal{R}_P$ ne se rencontrent pas, l'aire totale des parties qui se trouvent dans le carré est égale au nombre des $\mathcal{R}_P$ dans le carré multiplié par l'aire d'une d'entres elles (puisqu'elles sont toutes identiques), par exemple $\mathcal{R}_O$. Comme ces parties $\mathcal{R}_P$ sont toutes dans le carré de côté $2n+2d$, leur aire totale devrait être plus petite que celle du carré qui les contient, laquelle vaut $(2n+2d)^2$. Ce raisonnement géométrique se traduit par l'inégalité

$$\underbrace{(2n+1)^2}_{\text{nombre de } \mathcal{R}_P \text{ dans le carré}} \times \text{Aire}(\mathcal{R}_O) \leq \underbrace{(2n+2d)^2}_{\text{aire du carré}} ;$$

ce qui implique

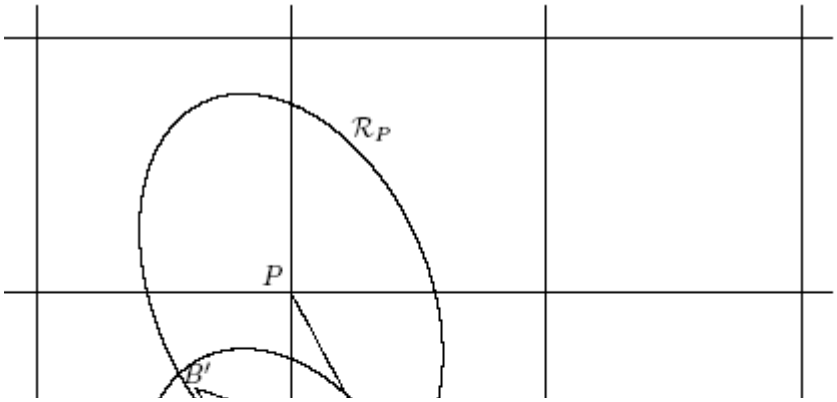
$$\text{Aire}(\mathcal{R}_O) \leq \left(\frac{2n+2d}{2n+1}\right)^2 .$$

Or le membre de droite dans la dernière inégalité tend vers 1, quand n devient grand. Cela peut se comprendre en remarquant que, lorsque n devient très grand, le « 2d » du numérateur et le « 1 » du dénominateur sont négligeables devant $2n$. Ainsi l'ordre de grandeur de *Unknown control sequence '\dfrac'*, quand n est très grand, est *Unknown control sequence '\dfrac'*, c'est-à-dire 1.

L'inégalité précédente montre donc que l'aire de $\mathcal{R}_O$ est plus petite que 1, voire lui est égale, ce qui est contraire à l'hypothèse de départ. Il est donc impossible qu'aucune des parties $\mathcal{R}_P$ n'en rencontre au moins une autre. Par conséquent, il existe deux points distincts du réseau Q et Q' pour lesquels les parties $\mathcal{R}_Q$ et $\mathcal{R}_{Q'}$ ont au moins un point en commun. On peut se ramener au cas où l'un de ces points est l'origine O. Nous noterons alors le second $P(p_1,p_2)$.

Il s'agit maintenant de justifier que le point P est précisément l'un de ceux que nous cherchions, c'est-à-dire que c'est un point du réseau qui se trouve dans $\mathcal{R}$. Pour cela, on vérifie que le milieu du segment $[OP]$, dont les coordonnées sont $(\frac{p_1}{2},\frac{p_2}{2})$, est un point de $\mathcal{R}_O$. C'est ici qu'il convient de se rappeler que $\mathcal{R}_O$ est de taille moitié de celle de $\mathcal{R}$ dans toutes les directions (voir la figure 7 pour suivre la fin du raisonnement).

Comme $\mathcal{R}_O$ et $\mathcal{R}_P$ ont des points en commun, soit $A(a_1,a_2)$ un point de $\mathcal{R}_O$ et $\mathcal{R}_P$. On construit un nouveau point $B(b_1,b_2)$ en prenant



$$b_1 = a_1 - p_1, \quad b_2 = a_2 - p_2;$$

B est tel que le $OBAP$ est un parallélogramme.

B appartient à $\mathcal{R}_O$ [15] et donc, comme $\mathcal{R}_O$ est symétrique par rapport à O, $B'(-b_1, -b_2)$ est aussi dans $\mathcal{R}_O$. $\mathcal{R}_O$ est convexe, par conséquent, elle contient le milieu C du segment joignant les points A et B'. Ce dernier point C a pour coordonnées $(\frac{a_1-b_1}{2}, \frac{a_2-b_2}{2})$, c'est-à-dire $(\frac{p_1}{2}, \frac{p_2}{2})$. Par définition de $\mathcal{R}_O = \frac{1}{2}\mathcal{R}$, on en déduit que le point $P(p_1, p_2)$ est bien un point du réseau qui est dans $\mathcal{R}$.

Il reste à traiter le cas où l'aire de $\mathcal{R}$ est exactement 4. On raisonne une nouvelle fois par l'absurde et on suppose qu'il n'y a aucun point du réseau à l'intérieur de $\mathcal{R}$ ou sur son bord. Cela signifie que tous les points du réseau sont situés au moins à une distance ε strictement positive du bord de $\mathcal{R}$. Sur cette base, on peut donc agrandir $\mathcal{R}$ de manière telle que les points du réseau soient encore tous à une distance au moins $\varepsilon/2$ du bord. Par ce biais, nous obtenons une partie qui vérifie les hypothèses du théorème, dont l'aire est strictement plus grande que 4 et qui ne contient aucun point du réseau dans son intérieur ou sur son bord. Mais cela contredit la première partie de la preuve du théorème. Le résultat de Minkowski est donc bien démontré.

Retour sur les formes quadratiques

Les conséquences de ce théorème de Minkowski sont très nombreuses. Dans un discours prononcé à la mort de Minkowski en 1909, Hilbert note la richesse de ses applications et parle, au sujet de la démonstration, de « perle de l'art heuristique de Minkowski ».

Pour obtenir de nouveaux résultats, il suffit d'appliquer le théorème à des parties convexes judicieusement choisies, ce que Minkowski fait dans des situations très variées. Pour l'illustrer, revenons à l'exemple des formes quadratiques binaires qui est à l'origine de son travail sur la géométrie des nombres. Soit $f(x, y) = ax^2 + 2bxy + cy^2$ une forme quadratique binaire définie positive. Cette hypothèse entraîne en particulier que la quantité $ac - b^2$ est strictement positive. On considère alors l'ensemble $\mathcal{E}$ des points du plan dont les coordonnées (x, y) vérifient

$$f(x, y) \leq k^2.$$

Cet ensemble est une ellipse, c'est donc bien une partie convexe et symétrique par rapport à l'origine. Il reste maintenant à choisir k^2 pour que l'aire de cette ellipse soit 4, on pourra alors appliquer le théorème de Minkowski. L'aire de $\mathcal{E}$ est $\frac{\pi k^2}{\sqrt{ac-b^2}}$, on pose donc $k^2 = \frac{4}{\pi}\sqrt{ac - b^2}$. D'après le théorème de Minkowski, il existe un couple d'entiers (m, n), différent de $(0, 0)$, tel que

$$f(m, n) = am^2 + 2bmn + cn^2 \leq \frac{4}{\pi}\sqrt{ac - b^2}.$$

Cette inégalité montre que la forme prend des valeurs plus petites que $\frac{4}{\pi}\sqrt{ac - b^2}$ quand ses

variables sont des entiers. Ceci est bien une solution à un problème décrit précédemment à propos des formes quadratiques.

Comme le théorème de Minkowski se généralise en dimension n quelconque, cette méthode permet de démontrer un résultat analogue pour les formes quadratiques définies positives de n variables [16]. L'avantage de la méthode de Minkowski est de donner une inégalité qui reste valable pour toutes les valeurs de n. Par contre, si l'entier n est fixé, elle ne conduit pas à la meilleure estimation. Par exemple, pour $n = 2$, la borne $\frac{4}{\pi}\sqrt{ac - b^2}$ peut être améliorée avec $\frac{2}{\sqrt{3}}\sqrt{ac - b^2}$ et les mathématiciens savaient déjà à l'époque de Minkowski qu'il s'agit de la meilleure constante possible (c'est-à-dire qu'il n'y a pas de borne plus petite qui donnerait une inégalité valable pour n'importe quelle forme quadratique binaire définie positive).

Actuellement, on ne connaît les constantes optimales que pour très peu de valeurs de n : pour $1 \leq n \leq 8$ et $n = 24$. Les méthodes employées pour les obtenir sont différentes de l'approche géométrique de Minkowski, mais c'est une autre histoire...

Bibliographie

Bayer-Fluckiger Eva, 2006, « Hermann Minkowski, Grand Prix de l'Académie à 18 ans », *Tangente* numéro 111, juillet-août 2006, pages 28-31.

Minkowski Hermann, 1896, *Geometrie der Zahlen*. Leipzig : Teubner.

Minkowski Hermann, 1911, *Gesammelte Abhandlungen*, volumes I et II. Édité par David Hilbert avec la collaboration de Andreas Speiser et Hermann Weyl, Leipzig : Teubner.

Nguyen Phong Q., 2008, « Une géométrie pour les prochains codes », *La Recherche* numéro 420, mai 2008.

Olds C.D., Lax Anneli et Davidoff Giuliana, 2000, *The Geometry of Numbers*. Washington : The Mathematical Association of America.

Notes

[▲1] On peut citer par exemple l'approximation diophantienne dont le problème est d'approcher des nombres réels ou complexes par des rationnels.

[▲2] Voir à ce sujet [Nguyen, 2008].

[▲3] Il s'agit maintenant de la ville de Kaunas en Lituanie.

[▲4] Dedekind est un mathématicien allemand connu en particulier pour ses travaux en théorie des nombres.

[▲5] Il s'agit de cours professés par Peter Gustav Lejeune-Dirichlet (mathématicien allemand) en 1856-1857 à Göttingen. Dedekind publie plusieurs éditions augmentées de ces cours entre 1863 et 1894.

[▲6] Les *Disquisitiones Arithmeticae*, publié par Carl Friedrich Gauss en 1801, est un livre de théorie des nombres qui eut une grande influence sur cette discipline par la suite. La section 5 de l'ouvrage est consacrée aux formes quadratiques binaires sur lesquelles nous reviendrons dans la suite.

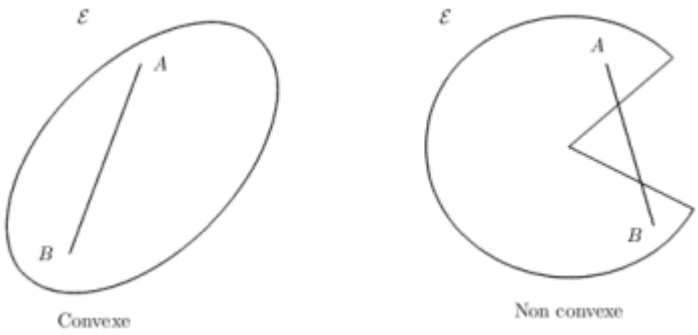
[▲7] Pour plus de détails sur l'attribution de ce prix, voir [Bayer-Fluckiger, 2006].

[▲8] Comme pour les formes binaires, une forme quadratique impliquant n variables peut s'écrire comme somme des carrés des variables et de produits des variables prises deux à deux (avec des coefficients).

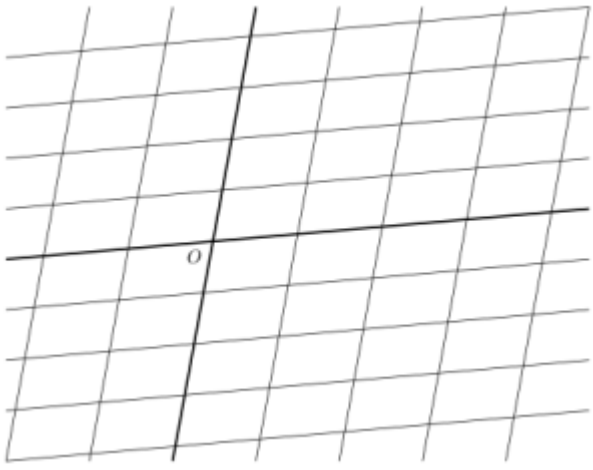
[▲9] Gauss propose aussi une notion de réduction pour les formes dites indéfinies, mais dans ce cas il n'y pas unicité de la forme réduite dans chaque classe.

[▲10] C'est-à-dire l'ensemble des points dont les coordonnées sont des nombres entiers.

[▲11] Un ensemble est convexe s'il contient chacun des segments qui joignent deux quelconques de ses points, voir la figure 2.



[▲12] Par exemple, dans le plan, on obtient un réseau en prenant deux droites sécantes, puis un ensemble des droites parallèles à chacune de ces deux sécantes. Les points d'intersection de ces droites sont les points du réseau. Il s'agit cette fois d'un quadrillage dont la maille est un parallélogramme, voir la figure 3.



[▲13] Même si les idées sont celles de Minkowski, les notations et la présentation ont été modifiées.

[▲14] Il s'agit de l'image de $\mathcal{R}$ par l'homothétie de centre O et de rapport $\frac{1}{2}$.

[▲15] En effet, $\mathcal{R}_O$ et $\mathcal{R}_P$ sont identiques à une translation de vecteur $\vec{OP}$ près, B est l'image de A

par cette translation et A appartient à $\mathcal{R}_O$.

[▲16] La borne obtenue par Minkowski pour une forme de n variables est $\frac{4}{\pi}\Gamma\left(1+\frac{n}{2}\right)^{2/n}|D|^{1/n}$, où D est une quantité qui ne dépend que des coefficients de la forme appelée discriminant ; dans le cas où $n=2, D=b^2-4ac$. La fonction Γ est définie pour $x>0$ par $\Gamma(x)=\int_0^{+\infty} t^{x-1}e^{-t}dt$.

Crédits images

Pour citer cet article : **Sébastien Gauthier**, **Hermann Minkowski : des formes quadratiques à la géométrie des nombres**. *Images des Mathématiques*, CNRS, 2009. En ligne, URL : **http://images.math.cnrs.fr/Hermann-Minkowski-des-formes,476.html**